



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/784,215	02/24/2004	Sampo Sovio	4208-4163 (NC28986)	8410
27123	7590	09/06/2007		
MORGAN & FINNEGAN, L.L.P. 3 WORLD FINANCIAL CENTER NEW YORK, NY 10281-2101			EXAMINER OKORONKWO, CHINWENDU C	
			ART UNIT 2136	PAPER NUMBER
			MAIL DATE 09/06/2007	DELIVERY MODE PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary

Application No.

10/784,215

Applicant(s)

SOVIO ET AL.

Examiner

Chinwendu C. Okoronkwo

Art Unit

2136

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 24 February 2004.
- 2a) ☐ This action is FINAL. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-84 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-84 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 24 February 2004 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
- ☐ Certified copies of the priority documents have been received.
 - ☐ Certified copies of the priority documents have been received in Application No. _____.
 - ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413) |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | Paper No(s)/Mail Date. _____ |
| 3) <input checked="" type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08) | 5) <input type="checkbox"/> Notice of Informal Patent Application |
| Paper No(s)/Mail Date <u>20040224</u> . | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

Priority

1. Applicant's claim for the benefit of a prior-filed application under 35 U.S.C. 119(a)-(e) or under 35 U.S.C. 120, 121, or 365(c) is acknowledged. Priority is claimed under Application 10662407.

Information Disclosure Statement

2. For the record, the Examiner acknowledges that the IDS submitted. It has been received and considered.

Oath/Declaration

3. For the record, the Examiner acknowledges that the Oath/Declaration submitted on 02/24/2004 has been received and considered.

Drawings

4. For the record, the Examiner acknowledges that the Drawings submitted on 02/24/2004 have been received and considered.

Specification

5. For the record, the Examiner acknowledges that the Specification submitted on 10/09/2003 has been received and considered.
6. Pursuant to USC 131, claims 1-80 are presented for examination.
7. Claims 1-80 are pending.

Claim Rejections - 35 USC § 103

8. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

Claims 1-80 are rejected under 35 U.S.C. 103(a) as being unpatentable over Halme et al. (US Patent Application Publication No.) and further in view of Kronenberg et al. (US Patent No.).

Regarding claims 1, 21 and 41, Halme et al., discloses a system for controlling data communication in an ad-hoc network that connects a wireless device and a nearby wireless device, comprising: a memory device (0115); and a processor disposed in communication with the memory device, the processor configured to: store an application directory having at least one entry, each entry including an application program identifier, attributes, and security parameters (0115); identify a selected entry based on the priority (0026); examine the attributes and the security parameters for the selected entry (0026-0027); and establish a security association to support the data communication when the security parameters direct the selected entry to use a secure connection (0030-0031).

Halme et al. is silent in disclosing determining a priority for each entry in the application directory, however Kronenberg does disclosure such elements (0055-0057 of Kronenberg).

It would have been obvious for one of ordinary skill in the art, at the time of the invention to have modified the processing of data packets within a network element cluster with the method and system for secured transport and storage of data on a network disclosed by Kronenberg. Motivation for this combination is taken from the Kronenberg recitation, "With the possibility of multiple IPsec tunnels there may also be multiple IPsec traffic, Secure Transport Traffic, SRNP traffic and Retrieval Datagram traffic on any relay. The ***Security Parameters Index (FIG. 5) field in the secure transport header datagrams can list unique identifiers necessary for the secure transport relay to identify the proper course of action for the packet.***"

Regarding claims 2, 22, and 42, Halme et al., discloses a system of claim 1, wherein the processor is further configured to: receive a connection request from the nearby wireless device (0036-0038); and send a first application directory to the nearby wireless device (0026-0027); and create the application directory by combining the first application directory and the second application directory (0026-0027).

Halme et al. is silent in disclosing receiving a second application directory from the nearby wireless device, however Kronenberg does disclose such elements (0055-0057 of Kronenberg).

It would have been obvious for one of ordinary skill in the art, at the time of the invention to have modified the processing of data packets within a network element cluster with the method and system for secured transport and storage of data on a network disclosed by Kronenberg. Motivation for this combination is taken from the Kronenberg recitation, "With the possibility of multiple IPsec tunnels there may also be multiple IPsec traffic, Secure Transport Traffic, SRNP traffic and Retrieval Datagram traffic on any relay. The ***Security Parameters Index (FIG. 5) field in the secure transport header datagrams can list unique identifiers necessary for the secure transport relay to identify the proper course of action for the packet.***"

Regarding claims 3, 23, and 43, Halme et al., discloses a system of claim 1, wherein the attributes include a device identifier, a role, and control parameters (0031-0033).

Regarding claims 4, 24 and 44, Halme et al., discloses a system of claim 3, wherein the control parameters include an application state, and at least one

user-defined application setting. (0041).

Regarding claims 5, 25 and 45, Halme et al., discloses a system of claim 1, wherein a bit-string includes the security parameters, a value of the bit-string representing each of the security parameters. (0063).

Regarding claims 6, 26 and 46, Halme et al., discloses system of claim 1, wherein the security parameters include an information security objective, a cryptography method for attaining the information security objective, and a level of security (0011-0013, 0019, 0043).

Regarding claims 7, 27 and 47, Halme et al., discloses a system of claim 6, wherein the information security objective includes maintaining confidentiality, ensuring integrity, authenticating a party, and protecting against replay or reuse (0074-0075).

Regarding claims 8, 28 and 48, Halme et al., discloses a system of claim 6, wherein the cryptography method includes a signature verification service, and an encryption algorithm (0011).

Regarding claims 9, 29 and 49, Halme et al., discloses a system of claim 6, wherein the level of security is a minimum required level of security (0005).

Regarding claims 10, 20 and 40, Halme et al., discloses a system of claim 1, wherein to determine the priority for each entry, the processor is further configured to: compare the attributes for each entry in said at least one entry (0095).

Regarding claims 11, 31 and 51, Halme et al., discloses a system of claim 1, wherein to establish the security association, the processor is further configured to: query a database for an existing security association between the wireless device and the nearby wireless device that will satisfy the security parameters; reuse the existing security association when the query of the database is successful; and create a new security association when the query of the database is unsuccessful (0012-0015).

Regarding claims 12, 32 and 52, Halme et al., discloses a system of claim 11, wherein the processor is further configured to: store the new security association in a connection log, wherein the query of the database includes examination of the connection log (0012-0015).

Regarding claims 13, 33 and 53, Halme et al., discloses a system of claim 11, wherein to reuse the existing security association, the processor is further configured to: notify the wireless device of the existing security association; notify

the nearby wireless device of the existing security association (0012-0015); launch an application program that is referenced by the application program identifier associated with the selected entry when the attributes associated with the selected entry indicate an accommodating state for the launch of the application program (0031-0033); and communicate over the secure connection with a counterpart application program on the nearby wireless device (0026-0027).

Regarding claims 14, 34 and 54, Halme et al., discloses a system of claim 11, wherein to create the new security association, the processor is further configured to: update the priority of the selected entry to defer the creating of the new security association (0071).

Regarding claims 15, 35 and 55, Halme et al., discloses a system of claim 11, wherein to create the new security association, the processor is further configured to: establish a privileged side channel to the nearby wireless device; negotiate the new security association over the privileged side channel; and store the new security association (0071).

Regarding claims 16, 36 and 56, Halme et al., discloses a system of claim 15, wherein the privileged side channel includes a proximity-based communication

means, including an infrared data association port, or a direct connection (0090-0091).

Regarding claims 17, 37 and 57, Halme et al., discloses a system of claim 15, wherein to negotiate the new security association, the processor is further configured to: send authentication data to the nearby wireless device (0012-00113); receive counterpart authentication data from the nearby wireless device (0033); and generate the new security association based on the authentication data and the counterpart authentication data (0071).

Regarding claims 18, 38 and 58, Halme et al., discloses a system of claim 1, wherein when the security parameters direct the selected entry to use a non-secure connection, the processor is further configured to: notify the wireless device of the non-secure connection (); notify the nearby wireless device of the non-secure connection (); launch an application program that is referenced by the application program identifier associated with the selected entry when the attributes associated with the selected entry indicate an accommodating state for the launch of the application program (); and communicate over the non-secure connection with a counterpart application program on the nearby wireless device (0075-0077).

Regarding claims 19, 39 and 59, Halme et al., discloses a system of claim 1, wherein the wireless device initiates the data communication (0091-0093).

Regarding claims 20, 30 and 50, Halme et al., discloses a system of claim 1, wherein the wireless device stores the application directory (0095).

Regarding claims 60 and 80, Halme et al., discloses a system of claim 51, wherein when the security parameters direct the selected entry to use a non-secure connection, further comprising: means for notifying the wireless device of the non-secure connection; means for notifying the nearby wireless device of the non-secure connection (0089-0091); means for launching an application program that is referenced by the application program identifier associated with the selected entry when the attributes associated with the selected entry indicate an accommodating state for the launch of the application program (0082); and means for communicating over the non-secure connection with a counterpart application program on the nearby wireless device (0089).

Regarding claims 61, 71 and 81, Halme et al., discloses a system for reconnecting to a secure connection in an ad-hoc network that connects a wireless device and a nearby wireless device, the wireless device storing an application directory having an entry that associates an application program on the wireless device to a counterpart application program on the nearby wireless

device, the entry including an application program identifier, attributes, and security parameters, comprising: a memory device; and a processor disposed in communication with the memory device, the processor configured to: store a security association between the wireless device and the nearby wireless device when the nearby wireless device enters the ad-hoc network for a first encounter; store a copy of the security association; remove the security association when the first encounter terminates; and establish a secure connection to the nearby wireless device based on the copy of the security association when the nearby wireless device enters the ad-hoc network for a second encounter (Rejected under the same rationale as claim 1).

Regarding claims 62, 72 and 82, Halme et al., discloses a system of claim 61, wherein the storing of the security association is to a short-term storage device (0071-0075).

Regarding claims 63, 73 and 83, Halme et al., discloses a system of claim 61, wherein the storing of the copy of the security association is to a long-term storage device (0071-0075).

Regarding claims 64, 74 and 84, Halme et al., discloses a system of claim 61, wherein to establish the secure connection to the nearby wireless device based on the copy of the security association when the nearby wireless device enters

the ad-hoc network for the second encounter, the processor is further configured to: search a connection log to locate the copy of the security association; launch the application program associated with the copy of the security association; configure the secure connection using the security parameters associated with the copy of the security association; and communicate over the secure connection with the counterpart application program (0026-0027).

Regarding claims 65 and 75, Halme et al., discloses a system of claim 64, wherein the processor is further configured to: verify that the copy of the security association will satisfy the security parameters for the second encounter (0055-0057).

Regarding claims 66 and 76, Halme et al., discloses a system of claim 64, wherein to search the connection log to locate the copy of the security association, the processor is further configured to: retrieve at least one previous connection from the connection log; and identify one of said at least one previous connection as the copy of the security association (0088-0089).

Regarding claims 67 and 77, Halme et al., discloses a method for reconnecting to a secure connection in an ad-hoc network that connects a wireless device and a nearby wireless device, the wireless device storing an application directory having an entry that associates an application program on the wireless device to

a counterpart application program on the nearby wireless device, the entry including an application program identifier, attributes, and security parameters, comprising: storing a security association between the wireless device and the nearby wireless device when the nearby wireless device enters the ad-hoc network for a first encounter; storing a copy of the security association; removing the security association when the first encounter terminates; and establishing a secure connection to the nearby wireless device based on the copy of the security association when the nearby wireless device enters the ad-hoc network for a second encounter (Rejected under the same rationale as claim 1).

Regarding claims 68 and 78, Halme et al., discloses a method of claim 67, wherein the storing of the security association is to a short-term storage device (0071-0075).

Regarding claims 69 and 79, Halme et al., discloses a method of claim 67, wherein the storing of the copy of the security association is to a long-term storage device (0071-0075).

Conclusion

9. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Chinwendu C. Okoronkwo whose telephone number is (571) 272 2662. The examiner can normally be reached on MWF 9:30 - 7:00.

Art Unit: 2136

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser Moazzami can be reached on (571) 272 4195. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

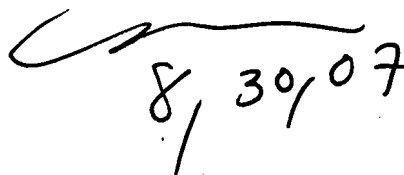
Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.



CCO

August 30, 2007

NASSER MOAZZAMI
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100



8/30/07